Strong Authentication in Intelligent Networks

Refik Molva
molva@eurecom.fr
Eurécom Institute
B.P. 193
06904 Sophia Antipolis - FRANCE

Pierre-Alain Etique
etique@tcom.epfl.ch

Jean-Pierre Hubaux
hubaux@tcom.epfl.ch

Telecommunications Laboratory
Swiss Federal Institute of Technology
CH-1015 Lausanne - SWITZERLAND

Abstract

The Intelligent Network (IN) architecture is designed to enable rapid deployment of new services in telecommunication networks. But the security of this architecture, and of the new services based on it, must be guaranteed. For example, it is likely that for sensitive services a simple PIN authentication will not be considered as secure enough by customers.

In this paper we propose a solution for a strong user authentication in an Intelligent Network, addressing the diversity of user terminal equipment. We present the necessary extensions of the Distributed Functional Plane (DFP), the associated cryptographic protocols, and the new Service Independent Building Blocks (SIB) which can be used for introducing strong authentication in a service specification.*

1 Introduction

The Intelligent Network (IN) architecture is designed to enable rapid deployment of new services in telecommunication networks [Q.1200]. But this architecture, as well as the new services based on it raise serious concern about the security of the subscribers and possible illegal access to the resources of the network and service providers.

Since the IN architecture includes at least three different types of players, that is, the network providers, the service providers and the subscribers, all possible scenarios including potential malicious or simply wrong behaviour by one of these players, with respect to another, should be considered.

On one hand we must consider the fact that in the IN philosophy, external parties get access to network entities. The IN infrastructure allows a service provider to access the Service Management System (SMS) and to download new services in the network. If no special care is taken those new services might constitute a potential threat for the correct operation of the network. But even with a careful policy, the service provider must at least be able to manage the data parameterizing the services he is offering. These management functions could even be delegated to the end customer himself. The NA6 group of the ETSI points out that "*[protection] against illegal or unauthorized access to personal data and management information ... [is] of particular significance in IN security*" [NA6-92].

These security aspects principally concern the behaviour of the network as seen by service providers and the network operators. A global approach to these problems of internal security is proposed in [Che89].

On the other hand, security can be provided as a set of services to end users. Some of the existing services obviously need security functions. The confidence in services like Wide Area Centrex or Credit Card Calling highly depends on the security level the service provider can furnish. A simple PIN-based authentication is too weak for most applications because of inherent exposure of the cleartext PIN values to several public components and the possibility of replay.

In this paper we propose a solution for a strong user authentication[1]. This solution covers the verification of users by the network as well as mutual authentication between users. The mutual authentication is clearly of interest for companies providing value added services via the telecommunication network and that require a good assurance on their customers' identity.

The authentication scheme presented in this paper can be used as a first step for a general security architecture addressing the internal security problems presented above, as well as other threats to communications between users of the network [Prof92].

2 Authentication requirements

In a typical IN service, 3 different entities are involved: the caller, the network (including the network and service providers) and the callee[2]. The protection of network and service resources from potential intrusion by subscribers requires the **authentication by the network** whereby a subscriber's (caller or callee) identity is verified by the network. Such a mechanism might in turn provide a one-way verification of subscribers by the network in case the subscriber trusts the identity of the network provider or a two-way or mutual verification in case the subscriber needs some assurance about the network provider's claimed identity. In some sensitive applications like financial operations whereby the communicating subscribers need to verify the identity of one

* This work was partially funded by the Swiss Telecom PTT

[1] strong authentication: authentication using cryptographic techniques

[2] We do not explicitely consider multi party calls, but the technique presented here could be applied in a such a situation.

another there is a requirement for **peer-to-peer authentication**. If the communicating subscribers trust the network in its vouching for the identity of one another, then a mechanism that provides the authentication of subscribers by the network will be sufficient also to fulfill the peer-to-peer authentication requirement. If the subscribers do not trust the network to corroborate for the identity of one another, then a direct peer-to-peer authentication mechanism that does not rely on the network is required. Like the authentication by the network, the peer-to-peer authentication can be performed in either one- or two-way.

The design presented in the next sections will address both the authentication by the network and the peer-to-peer authentication requirements.

3 Design Criteria

The design of the authentication mechanisms that can be introduced in the IN architecture will be governed by two different factors:

- the terminal capabilities: various alternatives in terms of the amount of cryptographic operations (encryption using symmetric or asymmetric algorithms, key generation, secret storage), the user interface (simple keypad, smartcard reader) and terminal signaling protocols (multifrequency, ISDN) through which authentication exchanges can be carried out should be taken into account.

- existing IN protocols: the authentication procedures should be carried out by existing distributed IN components and the authentication messages should be exchanged using the existing information flows between IN components. Thus only the authentication exchanges that minimize the amount of additional message interaction between IN components should be adopted.

D. Profos [Prof92] points out that acceptance of security features in IN will principally depend upon 2 factors:

1- Terminal price must be kept low.

2- The end user should not have to change the way he uses the network.

Considering these two points plus the security level we want to achieve, we limit ourselves to 3 alternatives considering the terminal equipment for an authentication:

1- the classical id + PIN-code (security: low; price: null; usage complexity: low).

2- Any terminal + stand-alone token card realizing the cryptographic functions. The user has to type in some information which he gets from the network e.g. as a voice message. He then gives the answer that can be read on the calculator's display back to the network via the terminal[3]. (security: high; price: middle to low; usage complexity: high).

3- ISDN terminal + smartcard reader. The communication with the network occurs via the D-channel using USER_INFO messages [Q.931]. Every concerned user has his own smartcard. (security: high; price: high; usage complexity: very low).

4 Authentication Entities in the Distributed Functional Plane

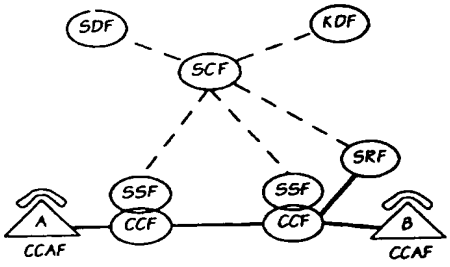
We will now analyze the mapping of main authentication entities onto the functional elements of the Distributed Functional Plane presented in the CCITT recommendation [Q.1200].

Both in the case of authentication by the network and the peer-to-peer authentication the subscriber is represented either by his smartcard, the token or the human user himself. In case of the authentication by the network, the subscriber should run an authentication protocol with an entity that verifies his identity on behalf of the network (or service provider). The DFP entity that is the most suitable for this role is the SCF since among all the functional entities the SCF is the only one that possesses the decision and control power.

In addition to the entities that are involved in the authentication as either the one that is authenticated or the one that is authenticating, authentication protocols call for a third party named key distribution center (KDC). When the authentication protocols are based on symmetric algorithms the KDC is in charge of generating and distributing pair-wise secrets that are used by the entities involved in the authentication. In case of authentication with public-key algorithms, the KDC generates public key certificates that provide any entity in the system with the tamper-proof information on the public key of any other entity. As opposed to the pair-wise secret keys, public key certificates do not vary with each execution of the authentication protocol, thus with a public-key based authentication system the KDC can be downgraded to a simple repository for public-key certificates generated in advance by some off-line process and for every possible entity in the system.

Like any other control function the SCF could also include the functions of the KDC but the design principles akin to secure systems call for the isolation of critical security functions in order to allow for their possible implementation by a dedicated physical component complying with stringent safety and security requirements. We thus suggest to represent the functions of the KDC by a new functional entity named key distribution function (KDF) as depicted in figure 1.

[3]The communication token -> network could be done directly if the token card is equipped with a DTMF sender.



CCAF: Call Control Access Function
A: caller; B: callee
CCF: Call Control Function
KDF: Key Distribution Function
SCF: Service Control Function
SDF: Service Data Function
SRF: Special Resource Function
SSF: Service Switching Function

Figure 1: The DFP extended for authentication

Each authentication procedure can involve an initiator named A representing the subscriber calling a service that requires authentication and possibly a responder named B representing the subscriber called through this service. The authentication scenarios in the DFP also involve the SCF representing the network or the service provider. The communication between the SCF and A or B does of course happen via the corresponding CCAF, SSF/CCF and an SRF accordingly to [Q.1200]. This scheme is fully identical to what happens for any user interaction in an IN-Service.

5 The protocols

For the sake of clarity the authentication protocols will be presented only in terms of cryptographic messages exchanged by the entities involved in authentication, that is the subscribers and the SCF as a representative of the network. The actual exchange of IN information flows and the lower layer messages that carry these will not be depicted.

Since the protocols are different depending on the capabilities of the terminal from which the user is calling or being called, the SCF must be able to determine the type of protocol to activate for each service instance. One can imagine several solutions to this problem. We could have a different service activation for each possible terminal capability. For example, prefix "171" would activate service "S" with a PIN authentication, whereby prefix "172" would activate "S" with token authentication and "173" would correspond to smartcard authentication. Another solution would be to ask the user in a classical "User Interaction" which authentication device is available.

5.1 Authentication by the network

PIN-Based

In the PIN-based verification case the protocol consists of sending the user's PIN in cleartext to the SCF. The PIN value is collected by the SCF through the usual "prompt and collect" [Q.1200] mechanism. This protocol thus offers the weakest security both from the point of view of the user and the network since the PIN value is exposed to numerous components (public terminals, exchanges, intelligent peripherals) and links traversed by the collect mechanism. Once a PIN value is spoofed by an intruder the impersonation of the legitimate user by the intruder is straightforward and requires even no special hardware or software arrangements.

Token Card-based

The protocol corresponding to the user equipped with a stand-alone token card is depicted in figure 2.

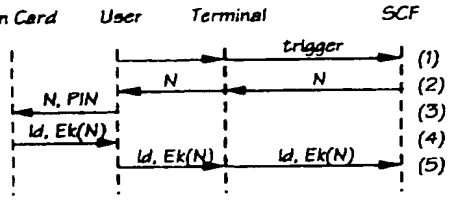


Figure 2: Authentication by the network using a token card

Flow 1 of this figure represents the trigger of the authentication service at the SCF by the standard IN mechanism. Each of the flows 2 and 5 is an abstraction of the usual "prompt and collect" mechanism defined in the IN standards. In flow 2 the SCF sends a freshly generated random number N to the terminal. The user obtains this number through the prompting capability (synthetic voice). In flow 3 the user enters N and his PIN into the token card using the keypad of the token card. The comparison of the PIN value entered by the user with the one stored in the card allows the token card to identify the user. This verification is not exposed to any eavesdropping or wiretapping or even any try-and-guess attack since this communication takes place through a strictly private channel; in case the card is stolen the number of unsuccessful tries before the card is locked out can be kept very low. Once the user is successfully identified by the token card, the card replies by displaying Ek(N) that is the encryption of N under the secret key K stored in the card. This message is entered by the user at the terminal based on the prompt and collect mechanism and reaches the SCF (flow 5). The SCF can then verify the identity of the user either by encrypting the stored value of N with the secret key K of the user and comparing the result with the value sent in flow 5 or by decrypting the latter with K and comparing the result with the stored value of N.

If the function E is not the encryption function of a full fledge encryption-decryption algorithm but only a **one-way function** then the verification based on encryption is mandatory. In order to verify the user's reply the SCF needs to know the user's key K. K can be stored in a safe repository along with the user name. A more elegant alternative eliminates the need for a repository commensurate with the number of users [Konig91]. In this alternative user U's key K is computed as Ekm(U), KM being the master key stored by the SCF and no other key being memorized by the SCF. Apart from the drawback of having the security of all users depend on the secrecy of a single key, this scheme offers the advantage of eliminating the burden of maintaining a safe key repository at the SCF.

Other alternatives to the previous protocol may easily be envisioned either by replacing the random number based challenge mechanism by a timestamp based mechanism that requires less interaction between the SCF and the terminal at the cost of synchronized clocks or by combining the PIN and the Ek(N) value at the terminal entry as in [Molva93].

Smartcard-based

Users equipped with a smartcard can use the protocol of figure 3 through terminals supporting a smartcard reader.

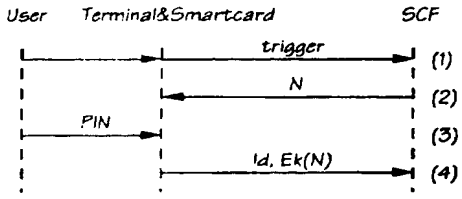


Figure 3: Authentication by the network using a smartcard

The main difference between this protocol and the token card based one is that in the smartcard case the exchange of the challenge (N) and the response take place directly between the personal device (smartcard) and the SCF through the communication channel. Another advantage of the smartcard scheme over the token card protocol is that public-key cryptography can be afforded both from the computing power point of view and regarding the feasibility aspects mainly because the lengthy messages (hundreds of digits) that would result from public key encryption in flow 4 would not cause any problem with respect to the communication between the terminal and the SCF as opposed to the token card case where reading and typing those numbers would exceed the capabilities and patience of normal human beings.

Both the smartcard and the token card based protocols can be extended to perform two-way authentication whereby the network is authenticated by the user (the smartcard or the token card) in addition to the user's authentication by the network. The authentication of the network is required when the possibility of the network provider's impersonation by Trojan attacks through "faked" public terminals or the possibility of call routing to an intruder system masquerading as the legitimate SCF should be taken into account.

Furthermore the protocols above are based on the assumption that the user and the SCF always share a secret key that identifies the user. Even though fairly realistic for most scenarios this assumption could be relaxed by the introduction of a key distribution function (KDF) that provides a user and the SCF he or she is communicating with with a shared key generated for the purpose of authentication without any need for a permanent shared key between the user and the SCF. Such key distribution protocols have been widely explored in the literature and an example of them is given in the next section. In case the authentication protocol is based on a public-key algorithm (RSA) instead of a symmetrical one (DES) the KDF might still be needed even though there is in this case no need for shared secret keys between the user and the SCF. The role of the KDF in the latter case is to provide each party with a public-key certificate proving that the public-key of the other party is valid and can be used in verifying the identity of the latter.

5.2 Peer-to-peer authentication

Peer-to-peer authentication can be obtained by the network mechanism if the peer entities (A and B) trust the network component (SCF) in its corroboration of one another. Otherwise a direct authentication protocol that does not rely on any network component is required. A direct peer-to-peer authentication mechanism heavily involves the terminal entities A and B and in the simplest case this protocol can be performed by A and B without any involvement of the network components as depicted in figure 4. Since this type of protocol is not specific to the IN architecture, any of the peer-to-peer authentication protocols presented in [Bird93], [Abadi89] and that are based on either random number challenges or timestamps can be used.

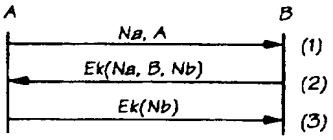


Figure 4: Peer-to-peer authentication

In order to execute such a protocol that requires encryption at both ends of the call, subscribers A and B need to have terminals equipped with smartcards. A solution using token cards can hardly be imagined (at least for two-way authentication) because of the high amount of interaction that would be required from the human user in order to exchange the protocol data back and forth between the terminal and the token card. A PIN based scheme can only be used for one-way authentication. A public-key version of this protocol can also easily be imagined as in [OSIDIR].

Nevertheless a peer-to-peer authentication protocol can benefit from the IN architecture in case of key distribution by a trusted key distribution center. The functions of the key distribution center can be represented by a key distribution function (KDF) in the DFP. The role of the KDF is to provide A and B with a shared secret key that is generated for the purpose of authentication in case of symmetrical cryptography (DES) or to distribute certificates for public-keys if asymmetrical cryptography is used.

Figure 5 depicts a sample key distribution protocol based on symmetric cryptography and random number challenges for authentication.

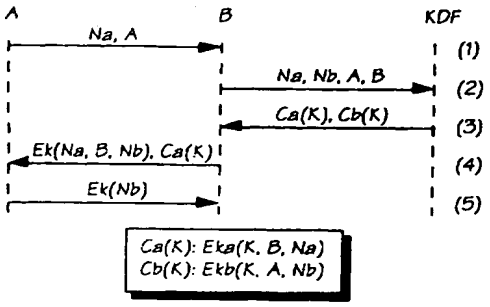


Figure 5: Key distribution supported by the network

In this protocol A and B initially share no secret key for authentication but with the KDF A shares key Ka and B key Kb. When A contacts B for authentication, B triggers a key distribution request to the KDF through the IN service interaction (flow 2) indicating the names of the subscribers that need the key to be distributed. KDF generates a new key K and encapsulates it in two different envelopes Ca(K) and Cb(K) destined respectively to A and to B. Since KDF stores in its key database the secret key of each subscriber it can compute such envelopes by encrypting the shared key K under the individual key of each destination entity. KDF's response (flow 3) is sent back to B through the IN interaction channels. B obtains key K by decrypting Cb(K) using its individual key Kb and forwards Ca(K) to A along with its authentication response Ek(Na,B,Nb) computed under the newly retrieved key K. A can get key K from Ca(K) using its secret key Ka and using K it can verify B's authentication response. If two-way authentication is required A can reply with the fifth flow containing A's response to the challenge (Nb) sent by B. Variations of similar key distribution protocols both for symmetrical and asymmetrical cryptography are widely explored in the literature [Needh78], [Abadi89], [Stein88], and [Molva92].[4]

6 New SIBs in the Global Functional Plane (GFP)

The GFP is the abstraction level in the IN Conceptual Model (INCM) [Q.1200] where the distributed aspects of the network are hidden and where services can be specified using Service Independent Building Blocks (SIBs) chained by a Global Service Logic (GSL) [Q.1200].

Our goal is to give a service developer the ability to introduce the authentication features presented above in his service specification. Therefore we introduce two new SIBs:

1- SIB "Authentication by IN" (figure 6). This SIB must be used if the service being defined requires the authentication of a subscriber by the network.

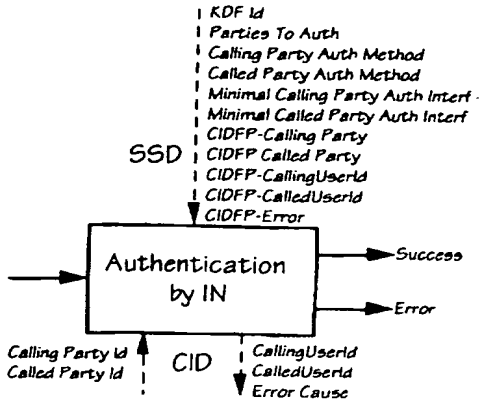


Figure 6: "Authentication by IN" SIB

Let us consider the three most important Service Support Data (SSD) that can be used to parameterize the SIB:

- **KDF Id:** This parameter identifies the key distribution center to be used allowing for the partitioning of the key distribution centers per service and per area. It is thus possible for a service provider to use its own key distribution center instead of a public one. It can be envisioned that even some service customers like banks, would not trust a public security service and require the provision of dedicated components for the implementation of critical functions like the KDF.

  Different key distribution servers of course call for different subscriber keys for each key server thus increasing the burden on safe key storage and key management on the subscriber side. This problem would be alleviated in case of public-key cryptography because in public-key based systems the key servers are downgraded to simple repositories.

- **Parties To Auth:** Possible values are *calling_party*, *called_party* and *both_parties*.

- **Minimal Calling Party Auth Interf:** Possible values are *PIN*, *Calculator*, *Smartcard*. It is considered that authentication by a PIN code is less secure than authentication with a calculator which itself is less secure than the use of a smartcard. Thus a service designer can decide that his service is too sensitive to allow PIN authentication, or even calculator authentication.

2- The second SIB is called "Authentication via IN" (figure 7). It represents the peer-to-peer authentication feature described in the previous sections. Only one SSD is new compared to the previous SIB:

- **Auth Method:** possible values are *one_way_AB* where the caller is authenticated by the callee, *one_way_BA* where the callee is authenticated by the

[4] A good design will choose the same protocol for user to network and for peer to peer authentication. That way it is possible to offer both services with the same user equipment.

caller and *two_way* where the caller and the callee mutually authenticate one another.

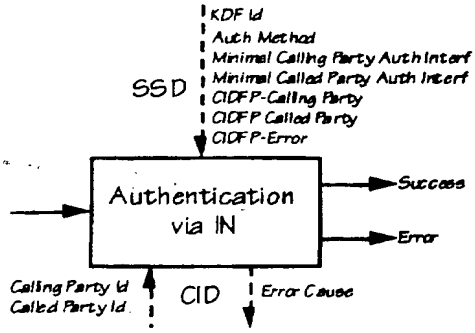


Figure 7: "Authentication via IN" SIB

Figure 8 shows an example service that could be described with the new SIBs. It shows how to build up a secure "Credit Card Calling" service: the account of the identified calling person is charged for the call instead of the account of the calling line.

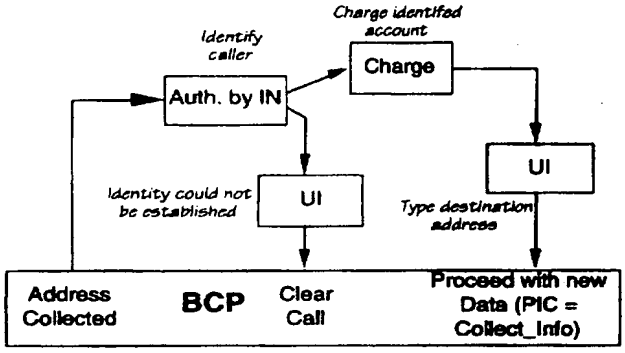


Figure 8: "Calling Person Charging" service.

7 Conclusions

In this paper we have shown how the Intelligent Network can be extended to allow strong authentication of users of the network. Basic authentication requirements relevant for the IN environment were identified as authentication by the network and peer-to-peer authentication. Three different terminal access interfaces have been taken into account: a smartcard and an ISDN terminal equipped with a card-reader, a hand held calculator which can be used with any type of terminal and the classical naked terminal used to enter an identity and a PIN code.

A set of authentication protocols fulfilling the two basic requirements in different terminal configurations were presented. Some of the issues related to key distribution and class of cryptographic algorithms were addressed.

We finally defined a presentation of these protocols in the service creation phase, by introducing two new SIBs that allow the specification of services requiring strong authentication as part of their normal operation.

Authentication is the first step towards a global security architecture in IN. Further study should focus on the provision of confidentiality, integrity, access control and security management functions by a security architecture integrated within the framework of IN.

Acknowledgments

We are grateful to Karim Berrah for his suggestions and ideas which greatly contributed to this paper.

References

[Abadi89] M. Burrows, M. Abadi, R. Needham, "A Logic of Authentication", Proc. of 12th ACM Symposium on Operating Systems, December 89.

[Bird93] R. Bird, P. Janson, S. Kutten, R. Molva, M. Yung,"Systematic Design of a Family of Attack-resistant Authentication Protocols", IEEE Journal on Selected Areas in Communications, June 1993.

[Che89] "Security Safeguards for Intelligent Networks", Che-Fn Yu, ICC89, Paper 37.3

[Konig91] H. Konigs "Cryptographic Identification Methods for Smart Cards in the Process of Standardization", IEEE Communications Magazine, June 1991

[Molva92] R. Molva, G. Tsudik, E. Van Herreweghen, S. Zatti, "KryptoKnight Authentication and Key Distribution System", Proc. of ESORICS 92, Toulouse- France

[Molva93] R. Molva, G. Tsudik,"Authentication Method with Impersonal Token Cards", Proc. of 1993 IEEE Symposium on Research in Security and Privacy, May 1993.

[NA6-92] "Report of WG3 / sub-group 4 meeting (Security IN)", TD48. Rev1, Annex 6 to Part B3 of the "Report of the 8th meeting of ETSI Sub-Technical Committee NA6 (Intelligent Networks) held in Rome, 7-11/9/1992

[Needh78] R. Needham, M. Schroeder, "Using Encryption for Authentication in Large Networks of Computers", Communications of the ACM, December 1978

[OSIDIR] "OSI Directory-Part 8: Authentication Framework", ISO Standard 9594-8, 1988.

[Prof92] "Security requirements and concepts for Intelligent Networks", D. Profos, International Zürich Seminar 1992, Paper A6

[Q.1200] Q.1200 - Q.1290 CCITT Study Group XI - Q.1200 Series "Intelligent Network", September 1992

[Q.931] "ISDN User-Network Interface Layer 3 Specification for Basic Call Control" CCITT Blue Book, Volume VI, Fascicle VI.11, Geneva 1989

[Stein88] J. G. Steiner, C. Neuman, J. I. Schiller, "Kerberos: an Authentication Server for Open Network Systems", Proc. of Usenix Conf. Winter 88.